

BEST AVAILABLE COPY
PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-283270

(43)Date of publication of application : 23.10.1998

(51)Int.CI.

G06F 12/14

G06F 9/06

H04L 9/32

(21)Application number : 09-091131

(71)Applicant : FUJITSU LTD

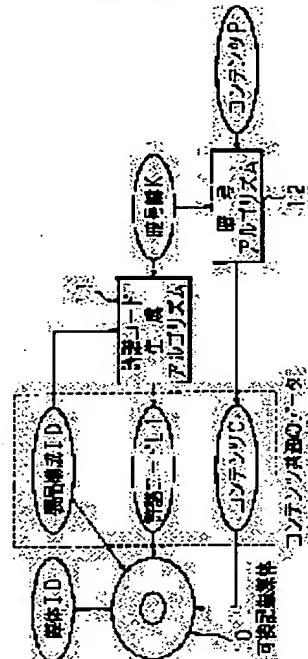
(22)Date of filing : 09.04.1997

(72)Inventor : YOSHIMOTO SHINICHI

(54) REPRODUCING PERMISSION METHOD, RECORDING METHOD, AND RECORDING MEDIUM**(57)Abstract:**

PROBLEM TO BE SOLVED: To provide a reproducing permission method which protects the copyright of information recorded in a recording medium without raising the production cost of the recording medium.

SOLUTION: Information (product constitution ID) peculiar to recording information (contents P) recorded in a recording medium 10 is used to encipher a first cipher key K to first encryption information (consent code L1), and the first cipher key is used to encipher recording information (contents P) to first encryption recording information (contents C), and peculiar information (product constitution ID) is recorded in a rewrite disableable area on the recording medium 10, and first encryption information (consent code L1) and first encryption recording information (contents C) are recorded in the rewritable area on the recording medium 10; and at the time of reproducing, read-out peculiar information (product constitution ID) is used to decode first encryption information (consent code L1) to the first cipher key K, and the decoded first cipher key is used to decode first encryption recording information (contents C) to recording information (contents P).

**LEGAL STATUS**

[Date of request for examination] 13.03.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3722584

[Date of registration] 22.09.2005

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-283270

(43)公開日 平成10年(1998)10月23日

(51)Int.Cl. ⁶	識別記号	F I
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14
9/06	5 5 0	9/06
H 0 4 L 9/32		H 0 4 L 9/00

3 2 0 F
3 2 0 B
5 5 0 Z
6 7 3 B
6 7 3 C

審査請求 未請求 請求項の数21 O L (全 23 頁)

(21)出願番号 特願平9-91131

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(22)出願日 平成9年(1997)4月9日

(72)発明者 吉本 真一

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74)代理人 弁理士 河野 登夫

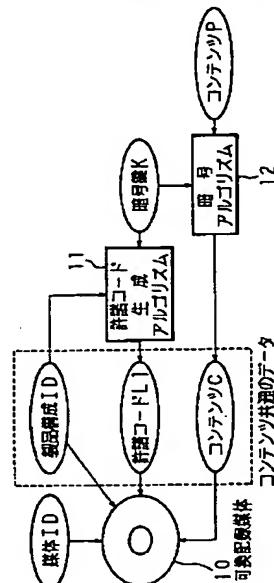
(54)【発明の名称】 再生許可方法、記録方法及び記録媒体

(57)【要約】

【課題】 記録媒体の製造コストの上昇を招くことなく、記録媒体に記録された情報の著作権を保護することができる再生許可方法の提供。

【解決手段】 記録媒体10に記録される記録情報(コンテンツP)に固有の情報(製品構成ID)を用いて第1の暗号鍵(暗号鍵K)を第1の暗号化情報(許諾コードL1)に暗号化し、第1の暗号鍵を用いて記録情報(コンテンツP)を第1の暗号化記録情報(コンテンツC)に暗号化し、固有の情報(製品構成ID)を記録媒体10上の書き換え不可能な領域に記録し、第1の暗号化情報(許諾コードL1)及び第1の暗号化記録情報(コンテンツC)を記録媒体10上の書き換え可能な領域に記録し、再生時には、読み出した固有の情報(製品構成ID)を用いて第1の暗号化情報(許諾コードL1)を第1の暗号鍵(暗号鍵K)に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報(コンテンツC)を記録情報(コンテンツP)に復号化する。

第1、2発明に係る再生許可方法、第11発明に係る記録方法
及び第14、15発明に係る記録媒体の実施の形態1を
説明するための説明図



【特許請求の範囲】

【請求項1】 記録媒体に記録されている記録情報又は複製された該記録情報の再生を、前記記録媒体に記録されている所定の情報を用いて、許可する再生許可方法において、

前記記録されている記録情報に固有の情報を前記記録媒体に記録し、前記記録情報の再生に前記固有の情報を必要とすることを特徴とする再生許可方法。

【請求項2】 記録媒体に記録される記録情報に固有の情報を用いて所定の第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて前記記録情報を第1の暗号化記録情報に暗号化し、前記固有の情報は前記記録媒体上の書き換え不可能な領域に記録し、第1の暗号化情報及び第1の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、

再生時には、読み出した前記固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報を復号化することを特徴とする再生許可方法。

【請求項3】 所定の第1の情報を用いて、記録媒体に記録されている記録情報又は複製された該記録情報の再生を許可する再生許可方法において、

前記記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を、前記記録情報の再生に必要とすることを特徴とする再生許可方法。

【請求項4】 前記固有の情報を用いて第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて前記記録情報を第1の暗号化記録情報に暗号化し、第1の暗号化情報及び第1の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、再生時には、前記固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報を復号化する請求項3記載の再生許可方法。

【請求項5】 前記固有の情報を用いて第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて前記記録情報を第1の暗号化記録情報に暗号化し、第1の暗号化情報及び第1の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、

最初の再生に先立って、前記固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を、所定の第2の情報を用いて第2の暗号化情報に暗号化し、第2の暗号化情報を第1の暗号化情報に替えて前記記録媒体上の書き換え可能な領域に記録し、再生時には、第2の情報を用いて第2の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報を復号化する請求項3記載の再生許可方法。

【請求項6】 前記固有の情報を用いて第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて前

記録情報を第1の暗号化記録情報に暗号化し、第1の暗号化情報及び第1の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、

最初の再生に先立って、前記固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報を復号化し、復号化した前記記録情報を、第2の暗号鍵を用いて第2の暗号化記録情報に暗号化し、所定の第2の情報を用いて第2の暗号鍵を第3の暗号化情報を暗号化し、第3の暗号化情報を第1の暗号化情報を替えて、

また、第2の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録し、再生時には、第2の情報を用いて第3の暗号化情報を第2の暗号鍵に復号化し、復号化した第2の暗号鍵を用いて第2の暗号化記録情報を前記記録情報を復号化する請求項3記載の再生許可方法。

【請求項7】 前記固有の情報を第1の暗号鍵に暗号化し、第1の暗号鍵を用いて前記記録情報を第1の暗号化記録情報を暗号化し、第1の暗号化記録情報は前記記録

媒体上の書き換え可能な領域に記録し、最初の再生に先立って、前記固有の情報を第1の暗号鍵に暗号化し、第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報を復号化し、所定の第2の情報を第2の暗号鍵に暗号化し、復号化した前記記録情報を、第2の暗号鍵を用いて第2の暗号化記録情報を暗号化し、第2の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録し、

再生時には、第2の情報を第2の暗号鍵に暗号化し、第2の暗号鍵を用いて第2の暗号化記録情報を前記記録情報を復号化する請求項3記載の再生許可方法。

【請求項8】 第2の情報は、前記記録媒体から読み出した前記記録媒体毎に固有の情報である請求項5～7の何れかに記載の再生許可方法。

【請求項9】 第2の情報は、ユーザ毎に固有の情報である請求項5～7の何れかに記載の再生許可方法。

【請求項10】 第2の情報は、前記ドライブ装置を制御するコンピュータに固有の情報である請求項5～7の何れかに記載の再生許可方法。

【請求項11】 記録する記録情報に固有の情報を用いて所定の第1の暗号鍵を第1の暗号化情報を暗号化し、第1の暗号鍵を用いて前記記録情報を第1の暗号化記録情報を暗号化し、前記固有の情報を書き換え不可能な領域に記録し、第1の暗号化情報及び第1の暗号化記録情報を書き換え可能な領域に記録することを特徴とする記録媒体への記録方法。

【請求項12】 ドライブ装置に記録されているドライブ装置に固有の情報を用いて第1の暗号鍵を第1の暗号化情報を暗号化し、記録する記録情報を第1の暗号鍵を用いて第1の暗号化記録情報を暗号化し、第1の暗号化情報及び第1の暗号化記録情報を書き換え可能な領域に

記録することを特徴とする記録媒体への記録方法。

【請求項13】 ドライブ装置に記録されているドライブ装置に固有の情報を第1の暗号鍵に暗号化し、第1の暗号鍵を用いて、記録する記録情報を第1の暗号化記録情報に暗号化し、第1の暗号化記録情報を書き換え可能な領域に記録することを特徴とする記録媒体への記録方法。

【請求項14】 請求項1に記載された再生許可方法に適用される記録媒体であって、

記録してある記録情報に固有の情報を記録してあることを特徴とする記録媒体。

【請求項15】 前記固有の情報を用いて所定の暗号鍵から暗号化された暗号化情報を記録してある請求項14記載の記録媒体。

【請求項16】 請求項4に記載された再生許可方法に適用される記録媒体であって、

ドライブ装置に記録されているドライブ装置に固有の情報を用いて所定の暗号鍵から暗号化された暗号化情報を記録してあることを特徴とする記録媒体。

【請求項17】 請求項2に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、

読み出した、前記記録情報に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化するステップと、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする記録媒体。

【請求項18】 請求項4に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、

前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化するステップと、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする記録媒体。

【請求項19】 請求項5に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、

最初の再生に先立って、前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化するステップと、復号化した第1の暗号鍵を、所定の第2の情報を用いて第2の暗号化情報を暗号化するステップと、第2の暗号化情報を第1の暗号化情報を替えて前記適用記録媒体上の書き換え可能な領域に記録するステップと、

再生時には、第2の情報を用いて第2の暗号化情報を第1の暗号鍵に復号化するステップと、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする記録媒体。

【請求項20】 請求項6に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、

10 最初の再生に先立って、前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化するステップと、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化するステップと、復号化した前記記録情報を、第2の暗号鍵を用いて第2の暗号化記録情報を暗号化するステップと、所定の第2の情報を用いて第2の暗号鍵を第3の暗号化情報を暗号化するステップと、第3の暗号化情報を第1の暗号化情報を替えて、また、第2の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録するステップと、

再生時には、第2の情報を用いて第3の暗号化情報を第2の暗号鍵に復号化するステップと、復号化した第2の暗号鍵を用いて第2の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする記録媒体。

【請求項21】 請求項7に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、

30 最初の再生に先立って、前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を第1の暗号鍵に暗号化するステップと、第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化するステップと、所定の第2の情報を第2の暗号鍵に暗号化するステップと、復号化した前記記録情報を、第2の暗号鍵を用いて第2の暗号化記録情報を暗号化するステップと、第2の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録するステップと、

再生時には、第2の情報を第2の暗号鍵に暗号化するステップと、第2の暗号鍵を用いて第2の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、著作権を保護する為に、DVD (Digital Video Disc)、CD-ROM及びMO (Magneto-Optical) 等の記録媒体に記録されている記録情報又は複製された記録情報の再生を許可する

50 再生許可方法、その方法に適用される記録媒体への記録

方法、その方法に適用される記録媒体及びその方法の実施に直接使用されるコンピュータプログラムを記録してある記録媒体に関するものである。

【0002】

【従来の技術】現在、記録媒体が備えている記録媒体毎に異なる固有の情報（媒体ID）を用いて、記録媒体に記録されているソフトウェア及びコンテンツ（記録情報、以下、コンテンツと記す）の著作権を保護する為の様々な再生許可方法が用いられている。図16、17は、従来の再生許可方法の一例を説明する為の説明図である。図16は、記録媒体にコンテンツを記録するときの説明図であり、この再生許可方法では、まず、暗号アルゴリズムを備えたハードウェア又はソフトウェア72を用いて、適当な暗号鍵KによりコンテンツPを暗号化し、暗号化したコンテンツCを記録媒体70に記録する。

【0003】次に、許諾コード生成アルゴリズムを備えたハードウェア又はソフトウェア71を用いて、媒体ID及び暗号鍵Kから許諾コードL0を生成し、コンテンツPの著作権所有者が保管する。ここでは、記録媒体70の媒体IDを暗号鍵として用いて、暗号鍵Kを暗号化し、許諾コードL0を生成してもよい。許諾コードL0は、コンテンツPの著作権所有者が、コンテンツPの使用を許可した者にのみ与えるものとする。

【0004】図17は、記録媒体70のコンテンツCを使用するときの説明図であり、コンテンツ使用者は、まず、コンテンツPの著作権所有者から使用許可を受け、許諾コードL0を得ることが必要である。許諾コードL0を得ることができた場合、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア73を用いて、媒体ID及び許諾コードL0から暗号鍵Kを得ることができる。媒体IDを暗号鍵として用いて、許諾コードL0を復号し、暗号鍵Kを得てもよい。コンテンツ使用者は、暗号鍵Kを得ることにより、復号アルゴリズムを備えたハードウェア又はソフトウェア74を用いて、暗号鍵K及び媒体IDにより、暗号化されたコンテンツCをコンテンツPに復号して使用することが可能となる。

【0005】この再生許可方法の特徴は、記録媒体70毎に異なる媒体IDを用いている為、コンテンツPを使用するには、コンテンツCが記録されている記録媒体70毎に許諾コードL0を必要とするところにある。例えば、記録媒体A用の許諾コードを持ったコンテンツ使用者が、コンテンツを記録媒体Aから記録媒体Bに複写し、記録媒体Bに複写したコンテンツを使用しようとして、記録媒体A用の許諾コードを用いたとしても、媒体IDが異なるため、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア73が正しい暗号鍵Kを生成することができず、コンテンツを正しく復号することができない。記録媒体Bに記録されたコンテンツを使用するには、記録媒体B用の許諾コードを必要とする。記

録媒体A用の許諾コードしか持たないコンテンツ使用者は、記録媒体A上でのみコンテンツの使用を許可されるのである。

【0006】さらに、この再生許可方法を応用すれば、以下のようない方法が可能である。媒体IDが付加された書き換え可能な可換記録媒体（DVD媒体、CD-ROM媒体、MO媒体等）の書き換え可能な領域に暗号化されたコンテンツを記録し、書き換え不可能な領域に許諾コードを記録したものを作成する。コンテンツ使用者は、可換記録媒体に記録されたコンテンツの使用料金をコンテンツの著作権所有者に支払い、その可換記録媒体を受け取る。コンテンツ使用者は、既に可換記録媒体に記録されている許諾コードを用いて、その可換記録媒体上のコンテンツを自由に使用できるが、その可換記録媒体から他の可換記録媒体へそのコンテンツを複写した場合、許諾コードは複写されないので、他の可換記録媒体上のコンテンツを正しく復号することはできない。

【0007】

【発明が解決しようとする課題】可換記録媒体は持ち運びが容易である為、上述した方法によりコンテンツ及び許諾コードが記録された可換記録媒体は、コンテンツ流通の手段として極めて有効である。しかし、この方法では、許諾コード及びコンテンツが記録された可換記録媒体を製造するのに大きなコストがかかる問題がある。

【0008】具体的には、可換記録媒体の製造工程において、媒体毎に変化する許諾コードを生成し、生成した許諾コードを対応する可換記録媒体に記録する等、一般的なCD-ROM等の製造設備より複雑な設備が必要となる。また、製造工程の後に行われる検査工程においても、可換記録媒体毎に許諾コードが異なるので、1枚ずつ可換記録媒体上の許諾コードが正しいか否かを検査しなければならず、その為、CD-ROMに較べて製造コストが高くなる。本発明は、前述したような事情に鑑みてなされたものであり、記録媒体の製造コストの上昇を招くことなく、記録媒体に記録された情報の著作権を保護することができる再生許可方法及び記録媒体を提供することを目的とする。

【0009】

【課題を解決するための手段】第1発明に係る再生許可方法は、記録媒体に記録されている記録情報又は複製された該記録情報の再生を、前記記録媒体に記録されている所定の情報を用いて、許可する再生許可方法において、前記記録されている記録情報に固有の情報を前記記録媒体に記録し、前記記録情報の再生に前記固有の情報を必要とすることを特徴とする。

【0010】この再生許可方法では、記録媒体に記録されている記録情報に固有の情報を記録媒体に記録し、記録情報の再生にその固有の情報を必要とするので、その固有の情報を読み出せた場合に限り、記録情報の再生を許可することができる。これにより、記録情報が同じで

ある記録媒体は、その他の内容構成も同一となるので、一括して製造、検査を行うことができ、製造コストの上昇を招くことなく、記録媒体に記録された情報の著作権を保護することができる。

【0011】第2発明に係る再生許可方法は、記録媒体に記録される記録情報に固有の情報を用いて所定の第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて前記記録情報を第1の暗号化記録情報に暗号化し、前記固有の情報は前記記録媒体上の書き換え不可能な領域に記録し、第1の暗号化情報及び第1の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、再生時には、読み出した前記固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報を復号化することを特徴とする。

【0012】この再生許可方法では、記録媒体に記録されている記録情報に固有の情報を用いて第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて記録情報を第1の暗号化記録情報に暗号化する。そして、記録情報に固有の情報は記録媒体上の書き換え不可能な領域に記録し、第1の暗号化情報及び第1の暗号化記録情報は記録媒体上の書き換え可能な領域に記録する。再生時には、読み出した記録情報に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を記録情報を復号化する。

【0013】これにより、別の記録媒体に複写した場合、記録情報に固有の情報は複写されないので、第1の暗号鍵が復号化できず、記録情報を再生できない。従って、記録媒体に記録されている記録情報の著作権を保護することができる。また、記録情報が同じである記録媒体は、その他の内容構成も同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0014】第3発明に係る再生許可方法は、所定の第1の情報を用いて、記録媒体に記録されている記録情報又は複製された該記録情報の再生を許可する再生許可方法において、前記記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を、前記記録情報の再生に必要とすることを特徴とする。

【0015】この再生許可方法では、記録媒体に記録されている記録情報の再生に、記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を必要とするので、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0016】第4発明に係る再生許可方法は、前記固有の情報を用いて第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて前記記録情報を第1の暗号化記録情報に暗号化し、第1の暗号化情報及び第1の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、再生時には、前記固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化することを特徴とする。

10 【0017】この再生許可方法では、ドライブ装置に固有の情報を用いて第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて記録情報を第1の暗号化記録情報に暗号化する。そして、第1の暗号化情報及び第1の暗号化記録情報は記録媒体上の書き換え可能な領域に記録する。再生時には、ドライブ装置に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を記録情報に復号化する。

20 【0018】これにより、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0019】第5発明に係る再生許可方法は、前記固有の情報を用いて第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて前記記録情報を第1の暗号化記録情報に暗号化し、第1の暗号化情報及び第1の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、最初の再生に先立って、前記固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を、所定の第2の情報を用いて第2の暗号化情報を暗号化し、第2の暗号化情報を第1の暗号化情報に替えて前記記録媒体上の書き換え可能な領域に記録し、再生時には、第2の情報を用いて第2の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化することを特徴とする。

40 【0020】この再生許可方法では、ドライブ装置に固有の情報を用いて第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて記録情報を第1の暗号化記録情報に暗号化する。そして、第1の暗号化情報及び第1の暗号化記録情報は記録媒体上の書き換え可能な領域に記録する。最初の再生に先立って、ドライブ装置に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を、所定の第2の情報を用いて第2の暗号化情報を暗号化する。そして、第2の暗号化情報を第1の暗号化情報に替えて記録媒体上の書き換え可能な領域に記録する。再生時には、第2の

50 の書き換え可能な領域に記録する。

情報を用いて第2の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を記録情報に復号化する。

【0021】これにより、最初の再生に先立つ暗号化情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報の変更後は、別の記録媒体に複写した場合に、第2の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0022】第6発明に係る再生許可方法は、前記固有の情報を用いて第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて前記記録情報を第1の暗号化記録情報に暗号化し、第1の暗号化情報及び第1の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、最初の再生に先立って、前記固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化し、復号化した前記記録情報を、第2の暗号鍵を用いて第2の暗号化記録情報を暗号化し、第2の情報を用いて第2の暗号鍵を第3の暗号化情報に暗号化し、第3の暗号化情報を第1の暗号化情報に替えて、また、第2の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録し、再生時には、第2の情報を用いて第3の暗号化情報を第2の暗号鍵に復号化し、復号化した第2の暗号鍵を用いて第2の暗号化記録情報を前記記録情報に復号化することを特徴とする。

【0023】この再生許可方法では、ドライブ装置に固有の情報を用いて第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて記録情報を第1の暗号化記録情報に暗号化する。そして、第1の暗号化情報及び第1の暗号化記録情報は記録媒体上の書き換え可能な領域に記録する。

【0024】最初の再生に先立って、ドライブ装置に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を記録情報に復号化する。復号化した記録情報は、第2の暗号鍵を用いて第2の暗号化記録情報を暗号化し、第2の情報を用いて第2の暗号鍵を第3の暗号化情報を暗号化する。そして、第3の暗号化情報を第1の暗号化情報に替えて、また、第2の暗号化記録情報を記録媒体上の書き換え可能な領域に記録する。再生時には、第2の情報を用いて第3の暗号化情報を第2の暗号鍵に復号化し、復号化した第2の暗号鍵を用いて第2の暗号化記録情報を記録情報に復号化する。

【0025】これにより、最初の再生に先立つ暗号化情報及び暗号化記録情報の変更を、ドライブ装置に固有の

情報が異なるドライブ装置では行えず、また、暗号化情報及び暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第2の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

10 【0026】第7発明に係る再生許可方法は、前記固有の情報を第1の暗号鍵に暗号化し、第1の暗号鍵を用いて前記記録情報を第1の暗号化記録情報を暗号化し、第1の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、最初の再生に先立って、前記固有の情報を第1の暗号鍵に暗号化し、第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報を復号化し、第2の情報を第2の暗号鍵に暗号化し、復号化した前記記録情報を、第2の暗号鍵を用いて第2の暗号化記録情報を暗号化し、第2の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録し、再生時には、第2の情報を第2の暗号鍵に暗号化し、第2の暗号鍵を用いて第2の暗号化記録情報を前記記録情報を復号化することを特徴とする。

20 【0027】この再生許可方法では、ドライブ装置に固有の情報を第1の暗号鍵に暗号化し、第1の暗号鍵を用いて記録情報を第1の暗号化記録情報を暗号化する。そして、第1の暗号化記録情報は記録媒体上の書き換え可能な領域に記録する。最初の再生に先立って、ドライブ装置に固有の情報を第1の暗号鍵に暗号化し、第1の暗号鍵を用いて第1の暗号化記録情報を記録情報に復号化する。そして、第2の情報を第2の暗号鍵に暗号化し、復号化した記録情報を、第2の暗号鍵を用いて第2の暗号化記録情報を暗号化し、第2の暗号化記録情報を記録媒体上の書き換え可能な領域に記録する。再生時には、第2の情報を第2の暗号鍵に暗号化し、第2の暗号鍵を用いて第2の暗号化記録情報を記録情報に復号化する。

30 【0028】これにより、最初の再生に先立つ暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第2の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号鍵により暗号化された暗号化記録情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

40 【0029】第8発明に係る再生許可方法は、第2の情報は、前記記録媒体から読み出した前記記録媒体毎に固有の情報を特徴とする。

【0030】この再生許可方法では、第2の情報は、記録媒体から読み出した記録媒体毎に固有の情報であるので、最初の再生に先立つ暗号化情報又は暗号化記録情報の変更後は、別の記録媒体に複写した場合に、記録媒体毎に固有の情報は複写されず、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【0031】第9発明に係る再生許可方法は、第2の情報は、ユーザ毎に固有の情報であることを特徴とする。

【0032】この再生許可方法では、第2の情報は、ユーザ毎に固有の情報であるので、最初の再生に先立つ暗号化情報又は暗号化記録情報の変更後は、別の記録媒体に複写した場合に、ユーザが異なれば、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【0033】第10発明に係る再生許可方法は、第2の情報は、前記ドライブ装置を制御するコンピュータに固有の情報であることを特徴とする。

【0034】この再生許可方法では、第2の情報は、ドライブ装置を制御するコンピュータに固有の情報であるので、最初の再生に先立つ暗号化情報又は暗号化記録情報の変更後は、別の記録媒体に複写した場合に、ドライブ装置を制御するコンピュータが異なれば、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【0035】第11発明に係る記録方法は、記録する記録情報に固有の情報を用いて所定の第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて前記記録情報を第1の暗号化記録情報に暗号化し、前記固有の情報を書き換え不可能な領域に記録し、第1の暗号化情報及び第1の暗号化記録情報を書き換え可能な領域に記録することを特徴とする。

【0036】この記録方法では、記録媒体に記録する記録情報に固有の情報を用いて第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて記録情報を第1の暗号化記録情報に暗号化する。そして、記録情報に固有の情報は記録媒体上の書き換え不可能な領域に記録し、第1の暗号化情報及び第1の暗号化記録情報は記録媒体上の書き換え可能な領域に記録する。これにより、別の記録媒体に複写した場合、記録情報に固有の情報は複写されないので、第1の暗号鍵が復号化できず、記録情報を再生できない。従って、記録媒体に記録されている記録情報の著作権を保護することができる。また、記録情報が同じである記録媒体は、その他の内容構成も同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0037】第12発明に係る記録方法は、ドライブ装置に記録されているドライブ装置に固有の情報を用いて第1の暗号鍵を第1の暗号化情報に暗号化し、記録する記録情報を第1の暗号鍵を用いて第1の暗号化記録情報

に暗号化し、第1の暗号化情報及び第1の暗号化記録情報を書き換え可能な領域に記録することを特徴とする。

【0038】この記録方法では、ドライブ装置に固有の情報を用いて第1の暗号鍵を第1の暗号化情報に暗号化し、第1の暗号鍵を用いて記録情報を第1の暗号化記録情報に暗号化する。そして、第1の暗号化情報及び第1の暗号化記録情報は記録媒体上の書き換え可能な領域に記録する。これにより、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。また、ドライブ装置に固有の同じ情報による暗号化情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0039】第13発明に係る記録方法は、ドライブ装置に記録されているドライブ装置に固有の情報を第1の暗号鍵に暗号化し、第1の暗号鍵を用いて、記録する記録情報を第1の暗号化記録情報に暗号化し、第1の暗号化記録情報を書き換え可能な領域に記録することを特徴とする。

【0040】この記録方法では、ドライブ装置に固有の情報を第1の暗号鍵に暗号化し、第1の暗号鍵を用いて記録情報を第1の暗号化記録情報に暗号化する。そして、第1の暗号化記録情報を記録媒体上の書き換え可能な領域に記録する。これにより、最初の再生に先立つ暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号鍵により暗号化された暗号化記録情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0041】第14発明に係る記録媒体は、請求項1に記載された再生許可方法に適用される記録媒体であって、記録してある記録情報に固有の情報を記録してあることを特徴とする。

【0042】この記録媒体では、記録情報に固有の情報を記録媒体に記録し、記録情報の再生にその固有の情報を必要としてあるので、その固有の情報を読み出せた場合に限り、記録情報の再生を許可することができる。これにより、記録情報が同じである場合は、その他の内容構成も同一となるので、一括して製造、検査を行うことができ、製造コストの上昇を招くことなく、記録された情報の著作権を保護することができる。

【0043】第15発明に係る記録媒体は、前記固有の情報を用いて所定の暗号鍵から暗号化された暗号化情報を記録してあることを特徴とする。

【0044】この記録媒体では、記録情報に固有の情報を用いて所定の暗号鍵から暗号化された暗号化情報を記

録しており、複写されても記録情報に固有の情報は複写されず、暗号化情報を暗号鍵に復号できないので、記録情報が同じであれば、その他の内容構成も同一となり、一括して製造、検査を行うことができ、製造コストの上昇を招くことなく、記録された情報の著作権を保護することができる。

【0045】第16発明に係る記録媒体は、請求項4に記載された再生許可方法に適用される記録媒体であって、ドライブ装置に記録されているドライブ装置に固有の情報を用いて所定の暗号鍵から暗号化された暗号化情報を記録してあることを特徴とする。

【0046】この記録媒体では、第1の暗号化情報及び第1の暗号化記録情報は書き換え可能な領域に記録しているので、再生時には、ドライブ装置に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化でき、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を記録情報に復号化できる。これにより、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0047】第17発明に係る記録媒体は、請求項2に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、読み出した、前記記録情報に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化するステップと、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする。

【0048】この記録媒体に記録してあるコンピュータプログラムにより制御されるコンピュータでは、適用記録媒体に記録されている記録情報を再生するときに、読み出した記録情報に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を記録情報に復号化する。これにより、別の記録媒体に複写した場合、記録情報に固有の情報は複写されないので、第1の暗号鍵が復号化できず、記録情報を再生できない。従って、記録媒体に記録されている記録情報の著作権を保護することができる。

【0049】第18発明に係る記録媒体は、請求項4に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化するステップと、復号化した第1の暗号鍵を用いて

第1の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする。

【0050】この記録媒体に記録してあるコンピュータプログラムにより制御されるコンピュータでは、適用記録媒体に記録されている記録情報を再生するときに、ドライブ装置に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を記録情報に復号化する。これにより、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。

【0051】第19発明に係る記録媒体は、請求項5に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、最初の再生に先立って、前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化するステップと、復号化した第1の暗号鍵を、所定の第2の情報を用いて第2の暗号化情報を暗号化するステップと、第2の暗号化情報を第1の暗号鍵に復号化するステップと、再生時には、第2の情報を用いて第2の暗号化情報を第1の暗号鍵に復号化するステップと、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする。

【0052】この記録媒体に記録してあるコンピュータプログラムにより制御されるコンピュータでは、適用記録媒体に記録されている記録情報の最初の再生に先立って、ドライブ装置に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を、所定の第2の情報を用いて第2の暗号化情報を暗号化する。そして、第2の暗号化情報を第1の暗号化情報を替えて記録媒体上の書き換え可能な領域に記録する。記録情報の再生時には、第2の情報を用いて第2の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を記録情報に復号化する。

【0053】これにより、最初の再生に先立つ暗号化情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報の変更後は、別の記録媒体に複写した場合に、第2の情報がなければ、記録情報を復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【0054】第20発明に係る記録媒体は、請求項6に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプロ

グラムを記録してある記録媒体であって、最初の再生に先立って、前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化するステップと、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化するステップと、復号化した前記記録情報を、第2の暗号鍵を用いて第2の暗号化記録情報に暗号化するステップと、所定の第2の情報を用いて第2の暗号鍵を第3の暗号化情報を暗号化するステップと、第3の暗号化情報を第1の暗号化情報を替えて、また、第2の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録するステップと、再生時には、第2の情報を用いて第3の暗号化情報を第2の暗号鍵に復号化するステップと、復号化した第2の暗号鍵を用いて第2の暗号化記録情報を前記記録情報を復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする。

【0055】この記録媒体に記録してあるコンピュータプログラムにより制御されるコンピュータでは、適用記録媒体に記録されている記録情報の最初の再生に先立って、ドライブ装置に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化し、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を記録情報に復号化する。復号化した記録情報は、第2の暗号鍵を用いて第2の暗号化記録情報を暗号化し、第2の情報を用いて第2の暗号鍵を第3の暗号化情報を暗号化する。そして、第3の暗号化情報を第1の暗号化情報を替えて、また、第2の暗号化記録情報を記録媒体上の書き換え可能な領域に記録する。記録情報の再生時には、第2の情報を用いて第3の暗号化情報を第2の暗号鍵に復号化し、復号化した第2の暗号鍵を用いて第2の暗号化記録情報を記録情報に復号化する。

【0056】これにより、最初の再生に先立つ暗号化情報及び暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報及び暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第2の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【0057】第21発明に係る記録媒体は、請求項7に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、最初の再生に先立って、前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を第1の暗号鍵に暗号化するステップと、第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報を復号化するステップと、所定の第2の情報を第2の暗号鍵に暗号化するステップと、復号化した前記記録情報を、第2の暗号鍵を用いて第2の暗号化記録情報を暗号化するステップと、第2の暗号

化記録情報を前記記録媒体上の書き換え可能な領域に記録するステップと、再生時には、第2の情報を第2の暗号鍵に暗号化するステップと、第2の暗号鍵を用いて第2の暗号化記録情報を前記記録情報を復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする。

【0058】この記録媒体に記録してあるコンピュータプログラムにより制御されるコンピュータでは、適用記録媒体に記録されている記録情報の最初の再生に先立って、ドライブ装置に固有の情報を第1の暗号鍵に暗号化し、第1の暗号鍵を用いて第1の暗号化記録情報を記録情報に復号化する。そして、第2の情報を第2の暗号鍵に暗号化し、復号化した記録情報を、第2の暗号鍵を用いて第2の暗号化記録情報を暗号化し、第2の暗号化記録情報を記録媒体上の書き換え可能な領域に記録する。記録情報の再生時には、第2の情報を第2の暗号鍵に暗号化し、第2の暗号鍵を用いて第2の暗号化記録情報を記録情報に復号化する。

【0059】これにより、最初の再生に先立つ暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第2の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【0060】

【発明の実施の形態】以下に、本発明をその実施の形態を示す図面に基づいて説明する。

実施の形態1. 図1は、第1、2発明に係る再生許可方法、第11発明に係る記録方法及び第14、15発明に係る記録媒体の実施の形態1を説明する為の説明図であり、書き換えが可能な可換記録媒体に記録する情報の生成方法を説明する為の説明図である。この生成方法は、可換記録媒体10(記録媒体)に記録するコンテンツ構成及び種類に対応する製品構成ID(記録情報に固有の情報)と、コンテンツP(記録情報)用の暗号鍵K(第1の暗号鍵)とから許諾コード生成アルゴリズムを備えたハードウェア又はソフトウェア11により、許諾コードL1(第1の暗号化情報)を生成する。製品構成ID及び可換記録媒体毎の媒体IDは、可換記録媒体10の書き換えが不可能な領域に記録する。

【0061】コンテンツP用の暗号鍵Kから暗号アルゴリズムを備えたハードウェア又はソフトウェア12により、コンテンツPを暗号化してコンテンツC(第1の暗号化記録情報)を生成し、前述した許諾コードL1と共に、可換記録媒体10の書き換えが可能な領域に記録する。

【0062】従来の再生許可方法(図16)では、媒体IDに依存した許諾コードL0を生成していたが、媒体ID毎に許諾コードL0を生成しなければならないの

で、製造設備が複雑になり、製造コストの上昇を招いていた。一方、図1に示した再生許可方法では、製品構成ID毎に許諾コードL1とコンテンツCとが共通のデータとなり、従来の再生許可方法(図16)より製造設備が簡単になり、製造コストを低く押さえることが可能となる。

【0063】図2は、可換記録媒体10に記録されたコンテンツCの利用方法を説明する為の説明図である。この利用方法では、可換記録媒体10から製品構成ID及び許諾コードL1を読み出し、暗号アルゴリズムを備えたハードウェア又はソフトウェア13を用いて、製品構成ID及び許諾コードL1から暗号鍵Kを得る。次に、得られた暗号鍵Kにより、復号アルゴリズムを備えたハードウェア又はソフトウェア14を用いて、暗号化されたコンテンツCをコンテンツPに復号する。これにより、コンテンツPを使用することが可能となる。

【0064】図3は、第1、2発明に係る再生許可方法に使用する可換記録媒体の製造工程を説明する為の説明図である。この製造工程では、まず、製造計画を立てる。製造計画では、可換記録媒体に記録するコンテンツの種類及び構成を決定し、このコンテンツの種類及び構成に対応する製品構成IDを決定して、コンテンツの種類及び構成と製品構成IDとの対応関係をメインコンピュータ80のデータベースに登録する。次いで、メインコンピュータ80により製造計画表を作成する。製造計画表には、製品構成ID、最初に製造される可換記録媒体の開始媒体ID及び製造枚数が記録されている。

【0065】製造開始に当たって、メインコンピュータ80は、製造計画表に従って、製造すべき可換記録媒体の製品構成IDと製造枚数を得、データベースサーバ81及びID記録機85に可換記録媒体製造の指示を出す。ID記録機85は、メインコンピュータ80から製造枚数、開始媒体ID及び製品構成IDを受け取り、開始媒体IDを媒体IDカウンタの初期値として設定する。次に、ID記録機85は、IDが記録されていない可換記録媒体84の書き換えが不可能な領域に、媒体IDカウンタが指示する媒体IDと製品構成IDとを記録する。媒体IDカウンタは、可換記録媒体84に媒体IDが記録される都度インクリメントされる。これにより、媒体IDと製品構成IDとが記録された可換記録媒体86を得ることができる。

【0066】一方、データベースサーバ81では、上述した方法(図1)により、コンテンツの暗号鍵を生成し、生成した暗号鍵を用いてコンテンツ群を暗号化する。このとき、暗号鍵と製品構成IDとの対応関係をデータベースに保存する。次に、製品構成IDに依存する許諾コードを生成する。これにより、可換記録媒体86に記録する全データ(暗号化されたコンテンツ群及び許諾コード)が決定され、この全データは複写機82に与えられる。複写機82では、暗号化されたコンテンツ群

及び許諾コードを、製造すべき枚数分の可換記録媒体86の書き換えが可能な領域に複写し、製品である可換記録媒体83を製造する。

【0067】実施の形態2、図4は、第3～5、8～10発明に係る再生許可方法、第12発明に係る記録方法及び第16発明に係る記録媒体の実施の形態2を説明する為の説明図であり、書き換えが可能な可換記録媒体に記録する情報の生成方法を説明する為の説明図である。この生成方法は、可換記録媒体用ドライブ装置メーカ21によって決められ、可換記録媒体用ドライブ装置に記録されているドライブID(ドライブ装置に固有の情報)と、コンテンツP(記録情報)用の暗号鍵K(第1の暗号鍵)とから許諾コード生成アルゴリズムを備えたハードウェア又はソフトウェア22により、許諾コードL1(第1の暗号化情報)を生成する。

【0068】コンテンツP用の暗号鍵Kから暗号アルゴリズムを備えたハードウェア又はソフトウェア23により、コンテンツPを暗号化してコンテンツC(第1の暗号化記録情報)を生成し、前述した許諾コードL1と共に、可換記録媒体20の書き換えが可能な領域に記録する。可換記録媒体毎の媒体ID(第2の情報、記録媒体毎に固有の情報)は、可換記録媒体20の書き換えが不可能な領域に記録する。

【0069】従来の再生許可方法(図16)では、媒体IDに依存した許諾コードL0を生成していたが、媒体ID毎に許諾コードL0を生成しなければならないので、製造設備が複雑になり、製造コストの上昇を招いていた。一方、図1に示した再生許可方法では、ドライブID毎に許諾コードL1とコンテンツCとが共通のデータとなり、従来の再生許可方法(図16)より製造設備が簡単になり、製造コストを低く押さえることが可能となる。

【0070】図5は、可換記録媒体20に記録されたコンテンツが初めて利用される前に行われる許諾コードの変更方法を説明する為の説明図である。コンテンツ使用者が可換記録媒体20に記録されたコンテンツCを利用するとき、可換記録媒体用ドライブ装置24は、まず、可換記録媒体20に記録されているコンテンツ利用情報を参照し、コンテンツが既に利用されているか否かを検査する。コンテンツが利用されていないときは、ドライブIDに依存する許諾コードL1を、媒体IDに依存する許諾コードL2(第2の暗号化情報)に変更する。

【0071】許諾コードL1から許諾コードL2への変更は以下のように行われる。可換記録媒体用ドライブ装置24から得られたドライブIDと、可換記録媒体20から読み出された許諾コードL1とから、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア25を用いて、暗号鍵Kを一時的に生成する。これにより、ドライブIDが異なる可換記録媒体用ドライブ装置では、暗号鍵Kを生成することができず、許諾コードの変

更を行なうことはできない。次に、許諾コード生成アルゴリズムを備えたハードウェア又はソフトウェア26を用いて、可換記録媒体20から読み出した媒体IDと暗号鍵Kとから、許諾コードL2を生成する。次に、得られた許諾コードL2を可換記録媒体20の書き換えが可能な領域に記録する。

【0072】許諾コードL2を可換記録媒体20に記録した後、可換記録媒体20上のコンテンツ利用情報を「コンテンツは既に利用された」の意味に変更する。これにより、以後、コンテンツ利用情報を参照することによって、「コンテンツは既に利用された」と判断され、許諾コードL2の再生成は行われない。これにより、可換記録媒体20から別の可換記録媒体に複写された場合でも、別の可換記録媒体の媒体IDにより、許諾コードL2が生成されることがないので、別の可換記録媒体に複写されたコンテンツが利用されることはない。

【0073】図6は、許諾コードL2が可換記録媒体20に記録された後に行われるコンテンツの復号過程を説明する為の説明図である。この復号過程では、まず、可換記録媒体20から媒体IDと許諾コードL2とを読み出す。次に、この媒体IDと許諾コードL2とから、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア27を用いて、暗号鍵Kを生成する。次に、暗号鍵Kから、復号アルゴリズムを備えたハードウェア又はソフトウェア28を用いて、コンテンツCをコンテンツPに復号する。これにより、コンテンツCの利用が可能となり、また、許諾コードの変更後は、ドライブIDが異なる可換記録媒体用ドライブ装置であっても、コンテンツCを利用することが可能となる。

【0074】尚、図5に示した許諾コードの変更を行わずに、実施の形態1の図2に示したように、直接、暗号化されたコンテンツCをコンテンツPに復号してもよい。但し、この場合は、製品構成IDに替えて、可換記録媒体用ドライブ装置24から得られたドライブIDを使用する。これにより、ドライブIDが異なる可換記録媒体用ドライブ装置では、コンテンツCを利用できなくなる。

【0075】本発明に係る再生許可方法の実施の形態2に使用する可換記録媒体の製造工程は、前述した本発明に係る再生許可方法の実施の形態1に使用する可換記録媒体の製造工程(図3)と略同様であるので、説明を省略する。但し、実施の形態2に使用する可換記録媒体の製造工程では、図3における製品構成IDに替わって、可換記録媒体用ドライブ装置メーカーによって決められたドライブIDであり、ID記録機85により記録されるIDは、媒体IDのみである。

【0076】実施の形態3、図7は、第3、6、8発明に係る再生許可方法及び第12発明に係る記録方法の実施の形態3に使用する可換記録媒体30に記録されたコンテンツが、初めて利用される前に行われる許諾コード

の変更方法及びコンテンツの再暗号化を説明する為の説明図である。書き換えが可能な可換記録媒体30に記録する情報の生成方法は、前述した実施の形態2において、図4を参照しながら説明した生成方法と同様であるので、説明を省略する。コンテンツ使用者が可換記録媒体30に記録されたコンテンツCを利用するとき、可換記録媒体用ドライブ装置31は、まず、可換記録媒体30に記録されているコンテンツ利用情報を参照し、コンテンツが既に利用されているか否かを検査する。コンテンツが利用されていないときは、ドライブIDに依存する許諾コードL1を、媒体IDに依存する許諾コードL2(第2の暗号化情報)に変更し、また、コンテンツC(第1の暗号化記録情報)を別の暗号アルゴリズムにより、コンテンツC2(第2の暗号化記録情報)に再暗号化する。

【0077】許諾コードL1から許諾コードL2への変更及びコンテンツCからコンテンツC2への再暗号化は、以下のように行われる。可換記録媒体用ドライブ装置31から得られたドライブIDと、可換記録媒体30から読み出された許諾コードL1とから、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア32を用いて、暗号鍵Kを一時的に生成する。これにより、ドライブIDが異なる可換記録媒体用ドライブ装置では、暗号鍵Kを生成することができず、許諾コードの変更及びコンテンツの再暗号化を行うことはできない。

【0078】一方、許諾コード生成アルゴリズムを備えたハードウェア又はソフトウェア34を用いて、可換記録媒体30から読み出した媒体IDと、暗号鍵Kではない別のコンテンツP用の暗号鍵K2(第2の暗号鍵)とから、許諾コードL2(第2の暗号化情報)を生成し、可換記録媒体30の書き換えが可能な領域に記録する。次に、順次、可換記録媒体30からコンテンツCを読み出し、復号アルゴリズムを備えたハードウェア又はソフトウェア33を用いて暗号鍵Kにより、コンテンツPへ復号し、復号したコンテンツPを、暗号アルゴリズムを備えたハードウェア又はソフトウェア35を用いて暗号鍵K2により、コンテンツC2へ再暗号化し、可換記録媒体30の書き換えが可能な領域に記録する。

【0079】許諾コードL2及び再暗号化したコンテンツC2を可換記録媒体30に記録した後、可換記録媒体30上のコンテンツ利用情報を「コンテンツは既に利用された」の意味に変更する。これにより、以後、コンテンツ利用情報を参照することによって、「コンテンツは既に利用された」と判断され、許諾コードL2の再生成は行われない。

【0080】これにより、可換記録媒体30から別の可換記録媒体に複写された場合でも、別の可換記録媒体の媒体IDにより、許諾コードL2が生成されることがなく、別の可換記録媒体に複写されたコンテンツが利用されることはない。また、許諾コードの変更及びコンテン

ツの再暗号化後は、ドライブIDが異なる可換記録媒体用ドライブ装置でも、可換記録媒体30を利用でき、コンテンツを読み出すことができる。

【0081】許諾コードL2が可換記録媒体30に記録された後に行われるコンテンツの復号過程は、前述した実施の形態2において、図6を参照しながら説明した復号過程と同様であるので、説明を省略する。但し、実施の形態3では、図6における暗号鍵K及びコンテンツCは、それぞれ暗号鍵K2及びコンテンツC2である。可換記録媒体30の製造工程は、前述した実施の形態1の可換記録媒体の製造工程(図3)と略同様であるので、説明を省略する。但し、可換記録媒体30の製造工程では、図3における製品構成IDに替わって、可換記録媒体用ドライブ装置メーカーによって決められたドライブIDであり、ID記録機85により記録されるIDは、媒体IDのみである。

【0082】実施の形態4、図8は、第3、7、8発明に係る再生許可方法及び第13発明に係る記録方法の実施の形態4を説明する為の説明図であり、書き換えが可能な可換記録媒体に記録する情報の生成方法を説明する為の説明図である。この生成方法は、可換記録媒体用ドライブ装置メーカー41によって決められ、可換記録媒体用ドライブ装置に記録されているドライブIDから、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア42を用いて、コンテンツP用の暗号鍵Kを生成する。

【0083】次に、コンテンツP用の暗号鍵Kから、暗号アルゴリズムを備えたハードウェア又はソフトウェア43を用いて、コンテンツPを暗号化してコンテンツCを生成し、可換記録媒体40の書き換えが可能な領域に記録する。可換記録媒体毎の媒体IDは、可換記録媒体20の書き換えが不可能な領域に記録する。

【0084】従来の再生許可方法(図16)では、媒体IDに依存した許諾コードL0を生成していたが、媒体ID毎に許諾コードL0を生成しなければならないので、製造設備が複雑になり、製造コストの上昇を招いていた。一方、図8に示した再生許可方法では、ドライブID毎にコンテンツCが共通のデータとなり、従来の再生許可方法(図16)より製造設備が簡単になり、製造コストを低く押さえることが可能となる。

【0085】図9は、可換記録媒体40に記録されたコンテンツが初めて利用される前に行われるコンテンツの再暗号化を説明する為の説明図である。コンテンツ使用者が可換記録媒体40に記録されたコンテンツCを利用するとき、可換記録媒体用ドライブ装置44は、まず、可換記録媒体40に記録されているコンテンツ利用情報を参照し、コンテンツが既に利用されているか否かを検査する。コンテンツが利用されていないときは、コンテンツCを別の暗号アルゴリズムにより、コンテンツC2に再暗号化する。

【0086】コンテンツCからコンテンツC2(第2の暗号化記録情報)への再暗号化は、以下のように行われる。可換記録媒体用ドライブ装置44から得られたドライブIDから、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア42を用いて、暗号鍵Kを一時的に生成する。これにより、ドライブIDが異なる可換記録媒体用ドライブ装置では、暗号鍵Kを生成することができず、許諾コードの変更及びコンテンツの再暗号化を行うことはできない。

10 【0087】一方、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア47を用いて、可換記録媒体40から読み出した媒体IDから、暗号鍵Kではない別のコンテンツP用の暗号鍵K2(第2の暗号鍵)を生成する。次に、順次、可換記録媒体40からコンテンツCを読み出し、復号アルゴリズムを備えたハードウェア又はソフトウェア46を用いて暗号鍵Kにより、コンテンツPへ復号し、復号したコンテンツPを、暗号アルゴリズムを備えたハードウェア又はソフトウェア48を用いて暗号鍵K2により、コンテンツC2へ再暗号化し、可換記録媒体40の書き換えが可能な領域に記録する。

【0088】再暗号化したコンテンツC2を可換記録媒体40に記録した後、可換記録媒体40上のコンテンツ利用情報を「コンテンツは既に利用された」の意味に変更する。これにより、以後、コンテンツ利用情報を参照することによって、「コンテンツは既に利用された」と判断され、コンテンツCからコンテンツC2への再暗号化は行われない。これにより、可換記録媒体40から別の可換記録媒体に複写された場合でも、別の可換記録媒体の媒体IDにより、暗号鍵K2が生成されることなく、別の可換記録媒体に複写されたコンテンツが利用されることはない。

【0089】図10は、再暗号化されたコンテンツC2が可換記録媒体40に記録された後に行われるコンテンツの復号過程を説明する為の説明図である。この復号過程では、まず、可換記録媒体40から媒体IDを読み出す。次に、この媒体IDから、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア49を用いて、暗号鍵K2を生成する。次に、暗号鍵K2から、復号アルゴリズムを備えたハードウェア又はソフトウェア50を用いて、コンテンツC2をコンテンツPに復号する。これにより、コンテンツCの利用が可能となり、また、許諾コードの変更及びコンテンツの再暗号化後は、ドライブIDが異なる可換記録媒体用ドライブ装置であっても、コンテンツCを利用することが可能となる。

【0090】本発明に係る再生許可方法の実施の形態4に使用する可換記録媒体の製造工程は、前述した本発明に係る再生許可方法の実施の形態1に使用する可換記録媒体の製造工程(図3)と略同様であるので、説明を省略する。但し、実施の形態4に使用する可換記録媒体の製造工程では、図3における製品構成IDに替わって、可

換記録媒体用ドライブ装置メーカーによって決められたドライブIDであり、ID記録機85により記録されるIDは、媒体IDのみである。また、複写機82により複写される情報は、暗号化されたコンテンツ群のみである。

【0091】実施の形態5. 図11は、第17発明に係る記録媒体の実施の形態の構成例を説明する為の説明図である。この実施の形態では、読み出した、前記記録情報に固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化するステップST10と、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化するステップST11とを含むコンピュータプログラムPR1を記録してあるCD-ROM(CD1)が、ディスクドライブDDに装填され、その内容はパソコンコンピュータPCに読み込まれる。

【0092】コンピュータプログラムPR1が読み込まれた後は、CD-ROM(CD1)はディスクドライブDDから取り出され、ディスクドライブDDには、例えば、可換記録媒体10(図1)が装填され、その内容がパソコンコンピュータPCに読み込まれる。パソコンコンピュータPCのその他の動作は、実施の形態1で説明したコンテンツCの利用方法と同様であるので、説明を省略する。

【0093】実施の形態6. 図12は、第18発明に係る記録媒体の実施の形態の構成例を説明する為の説明図である。この実施の形態では、ディスクドライブDD(適用記録媒体用ドライブ装置)に記録されているディスクドライブDDに固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化するステップST20と、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化するステップST21とを含むコンピュータプログラムPR2を記録してあるCD-ROM(CD2)が、ディスクドライブDDに装填され、その内容はパソコンコンピュータPCに読み込まれる。

【0094】コンピュータプログラムPR2が読み込まれた後は、CD-ROM(CD2)はディスクドライブDDから取り出され、ディスクドライブDDには、例えば、可換記録媒体20(図4)が装填され、その内容がパソコンコンピュータPCに読み込まれる。パソコンコンピュータPCのその他の動作は、実施の形態2で説明したコンテンツCの利用方法と同様であるので、説明を省略する。

【0095】実施の形態7. 図13は、第19発明に係る記録媒体の実施の形態の構成例を説明する為の説明図である。この実施の形態では、最初の再生に先立って、ディスクドライブDD(前記適用記録媒体用ドライブ装置)に記録されているディスクドライブDDに固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化するステップST30と、復号化した第1の暗号鍵を、所定の第2の情報を用いて第2の暗号化情報を暗号化する

ステップST31と、第2の暗号化情報を第1の暗号化情報に替えて前記適用記録媒体上の書き換え可能な領域に記録するステップST32と、再生時に、第2の情報を用いて第2の暗号化情報を第1の暗号鍵に復号化するステップST33と、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化するステップST34とを含むコンピュータプログラムPR3を記録してあるCD-ROM(CD3)が、ディスクドライブDDに装填され、その内容はパソコンコンピュータPCに読み込まれる。

【0096】コンピュータプログラムPR3が読み込まれた後は、CD-ROM(CD3)はディスクドライブDDから取り出され、ディスクドライブDDには、例えば、可換記録媒体20(図4)が装填され、その内容がパソコンコンピュータPCに読み込まれる。パソコンコンピュータPCのその他の動作は、実施の形態2で説明したコンテンツCの利用方法と同様であるので、説明を省略する。

【0097】実施の形態8. 図14は、第20発明に係る記録媒体の実施の形態の構成例を説明する為の説明図である。この実施の形態では、最初の再生に先立って、ディスクドライブDD(前記適用記録媒体用ドライブ装置)に記録されているディスクドライブDDに固有の情報を用いて第1の暗号化情報を第1の暗号鍵に復号化するステップST40と、復号化した第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化するステップST41と、復号化した前記記録情報を、第2の暗号鍵を用いて第2の暗号化記録情報を暗号化するステップST42と、所定の第2の情報を用いて第2の暗号鍵を第3の暗号化情報に暗号化するステップST43

と、第3の暗号化情報を第1の暗号化情報に替えて、また、第2の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録するステップST44と、再生時に、第2の情報を用いて第3の暗号化情報を第2の暗号鍵に復号化するステップST45と、復号化した第2の暗号鍵を用いて第2の暗号化記録情報を前記記録情報に復号化するステップST46とを含むコンピュータプログラムPR4を記録してあるCD-ROM(CD4)が、ディスクドライブDDに装填され、その内容はパソコンコンピュータPCに読み込まれる。

【0098】コンピュータプログラムPR4が読み込まれた後は、CD-ROM(CD4)はディスクドライブDDから取り出され、ディスクドライブDDには、例えば、可換記録媒体30(図7)が装填され、その内容がパソコンコンピュータPCに読み込まれる。パソコンコンピュータPCのその他の動作は、実施の形態3で説明したコンテンツCの利用方法と同様であるので、説明を省略する。

【0099】実施の形態9. 図15は、第21発明に係る記録媒体の実施の形態の構成例を説明する為の説明図

である。この実施の形態では、最初の再生に先立って、ディスクドライブDD（前記適用記録媒体用ドライブ装置）に記録されているディスクドライブDDに固有の情報を第1の暗号鍵に暗号化するステップST50と、第1の暗号鍵を用いて第1の暗号化記録情報を前記記録情報に復号化するステップST51と、所定の第2の情報を第2の暗号鍵に暗号化するステップST52と、復号化した前記記録情報を、第2の暗号鍵を用いて第2の暗号化記録情報を暗号化するステップST53と、第2の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録するステップST54と、再生時に、第2の情報を第2の暗号鍵に暗号化するステップST55と、第2の暗号鍵を用いて第2の暗号化記録情報を前記記録情報に復号化するステップST56とを含むコンピュータプログラムPR5を記録してあるCD-ROM(CD5)が、ディスクドライブDDに装填され、その内容はパソコン用コンピュータPCに読み込まれる。

【0100】コンピュータプログラムPR5が読み込まれた後は、CD-ROM(CD5)はディスクドライブDDから取り出され、ディスクドライブDDには、例えば、可換記録媒体40(図8)が装填され、その内容がパソコン用コンピュータPCに読み込まれる。パソコン用コンピュータPCのその他の動作は、実施の形態4で説明したコンテンツCの利用方法と同様であるので、説明を省略する。

【0101】尚、図5では、ドライブIDに依存した許諾コードL1から、媒体IDに依存した許諾コードL2へ変更する方法を示したが、媒体IDの替わりに、コンテンツ使用者毎に固有の情報に依存した許諾コードに変更してもよい。コンテンツ使用者毎に固有の情報とは、具体的には、コンピュータのOSが管理しているユーザID又はICカードに記録されているユーザID等である。その結果、可換記録媒体20に記録されたコンテンツは、特定のコンピュータ又は特定のユーザによる以外に利用することができなくなる。

【0102】また、媒体IDに依存した許諾コード、又はユーザ毎に固有の情報に依存した許諾コードの他に、可換記録媒体用ドライブ装置を制御するコンピュータに固有の情報に依存した許諾コードに変更してもよい。コンピュータに固有の情報とは、具体的には、コンピュータのBIOS(Basic Input Output System)が有するマシンID等である。その結果、可換記録媒体に記録されたコンテンツは、特定のコンピュータによる以外に利用することができなくなる。このように、許諾コードをどのような情報に依存させるかによって、様々なコンテンツ使用範囲を設定することができるが、これらは、コンテンツの著作権所有者に委ねられる。また、実施の形態5～9に記述した記録媒体は、CD-ROMに限らずハードディスク又は可換記録媒体等であっても良いことは言うまでもない。

【0103】

【発明の効果】第1発明に係る再生許可方法によれば、記録情報が同じである記録媒体は、一括して製造、検査を行うことができ、製造コストの上昇を招くことなく、記録媒体に記録された情報の著作権を保護することができる。

【0104】第2発明に係る再生許可方法によれば、別の記録媒体に複写した場合、記録情報に固有の情報は複写されないので、第1の暗号鍵が復号化できず、記録情報を復号化できない。従って、記録媒体に記録されている記録情報の著作権を保護することができる。また、記録情報が同じである記録媒体は、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0105】第3発明に係る再生許可方法によれば、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0106】第4発明に係る再生許可方法によれば、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0107】第5発明に係る再生許可方法によれば、最初の再生に先立つ暗号化情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報の変更後は、別の記録媒体に複写した場合に、第2の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0108】第6発明に係る再生許可方法によれば、最初の再生に先立つ暗号化情報及び暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報及び暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第2の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0109】第7発明に係る再生許可方法によれば、最

初の再生に先立つ暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第2の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号鍵により暗号化された暗号化記録情報を記録される記録媒体は、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0110】第8発明に係る再生許可方法によれば、最初の再生に先立つ暗号化情報又は暗号化記録情報の変更後は、別の記録媒体に複写した場合に、記録媒体毎に固有の情報は複写されず、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【0111】第9発明に係る再生許可方法によれば、最初の再生に先立つ暗号化情報又は暗号化記録情報の変更後は、別の記録媒体に複写した場合に、ユーザが異なれば、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【0112】第10発明に係る再生許可方法によれば、最初の再生に先立つ暗号化情報又は暗号化記録情報の変更後は、別の記録媒体に複写した場合に、ドライブ装置を制御するコンピュータが異なれば、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【0113】第11発明に係る記録方法によれば、別の記録媒体に複写した場合、記録情報に固有の情報は複写されないので、第1の暗号鍵が復号化できず、記録情報を再生できない。従って、記録媒体に記録されている記録情報の著作権を保護することができる。また、記録情報が同じである記録媒体は、その他の内容構成も同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0114】第12発明に係る記録方法によれば、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。また、ドライブ装置に固有の同じ情報による暗号化情報を記録される記録媒体は、その他の内容構成も同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0115】第13発明に係る記録方法によれば、最初の再生に先立つ暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えないで、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号鍵により暗号化された暗号化記録情報を記録さ

れる記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0116】第14、15発明に係る記録媒体によれば、記録情報が同じであれば、一括して製造、検査を行うことができ、製造コストの上昇を招くことなく、記録された情報の著作権を保護することができる。

【0117】第16発明に係る記録媒体によれば、ドライブ装置に固有の情報が異なるドライブ装置による再生

10 行えず、記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【0118】第17発明に係る記録媒体が記録しているプログラムにより制御されるコンピュータによれば、別の記録媒体に複写した場合、記録情報に固有の情報は複写されないので、第1の暗号鍵が復号化できず、記録情報を再生できない。従って、記録媒体に記録されている記録情報の著作権を保護することができる。

20 【0119】第18発明に係る記録媒体が記録しているプログラムにより制御されるコンピュータによれば、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。

【0120】第19発明に係る記録媒体が記録しているプログラムにより制御されるコンピュータによれば、最初の再生に先立つ暗号化情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報の変更後は、別の記録媒体に複写した場合に、第2の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

30 【0121】第20発明に係る記録媒体が記録しているプログラムにより制御されるコンピュータによれば、最初の再生に先立つ暗号化情報及び暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報及び暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第2の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

40 【0122】第21発明に係る記録媒体が記録しているプログラムにより制御されるコンピュータによれば、最初の再生に先立つ暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第2の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【図面の簡単な説明】

【図1】第1、2発明に係る再生許可方法、第11発明に係る記録方法及び第14、15発明に係る記録媒体の実施の形態1を説明する為の説明図である。

【図2】可換記録媒体に記録されたコンテンツの利用方法を説明する為の説明図である。

【図3】可換記録媒体の製造工程を説明する為の説明図である。

【図4】第3～5、8～10発明に係る再生許可方法、第12発明に係る記録方法及び第16発明に係る記録媒体の実施の形態2を説明する為の説明図である。

【図5】可換記録媒体に記録されたコンテンツが初めて利用される前に行われる許諾コードの変更方法を説明する為の説明図である。

【図6】許諾コードL2が可換記録媒体に記録された後に行われるコンテンツの復号過程を説明する為の説明図である。

【図7】許諾コードの変更方法及びコンテンツの再暗号化を説明する為の説明図である。

【図8】第3、7、8発明に係る再生許可方法及び第13発明に係る記録方法の実施の形態4を説明する為の説明図である。

【図9】可換記録媒体に記録されたコンテンツが初めて利用される前に行われるコンテンツの再暗号化を説明する為の説明図である。

【図10】再暗号化されたコンテンツが可換記録媒体に記録された後に行われるコンテンツの復号過程を説明する為の説明図である。

* 【図11】第17発明に係る記録媒体の実施の形態の構成を説明する為の説明図である。

【図12】第18発明に係る記録媒体の実施の形態の構成を説明する為の説明図である。

【図13】第19発明に係る記録媒体の実施の形態の構成を説明する為の説明図である。

【図14】第20発明に係る記録媒体の実施の形態の構成を説明する為の説明図である。

【図15】第21発明に係る記録媒体の実施の形態の構成を説明する為の説明図である。

【図16】従来の再生許可方法の一例を説明する為の説明図である。

【図17】従来の再生許可方法の一例を説明する為の説明図である。

【符号の説明】

10 10, 20, 30, 40 記録媒体（適用記録媒体）

11, 22, 26, 34 許諾コード生成アルゴリズムを備えたハードウェア又はソフトウェア

12, 23, 35, 43, 48 暗号アルゴリズムを備えたハードウェア又はソフトウェア

13, 25, 27, 32, 42, 47, 49 暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア

14, 28, 33, 46, 50 復号アルゴリズムを備えたハードウェア又はソフトウェア

CD1～CD5 CD-ROM（記録媒体）

DD ディスクドライブ

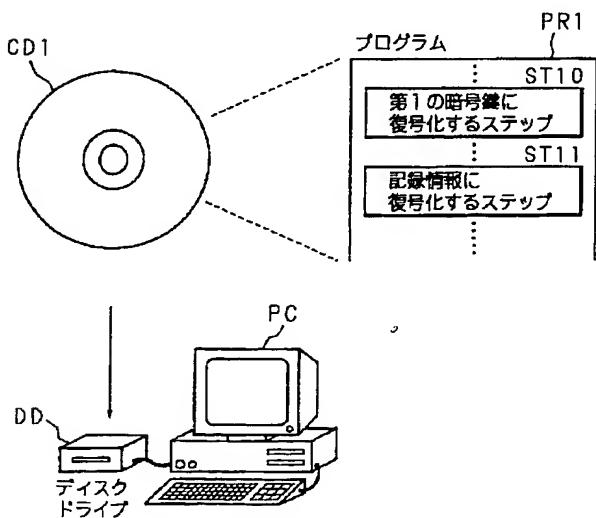
PR1～PR5 コンピュータプログラム

PC パーソナルコンピュータ（コンピュータ）

*

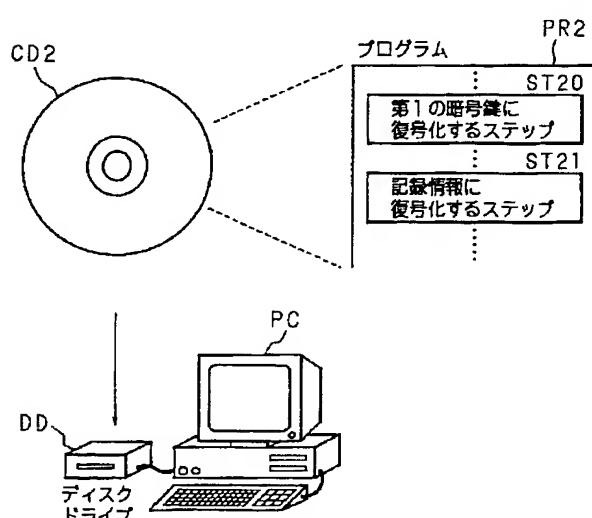
【図11】

第17発明に係る記録媒体の実施の形態の構成を説明する為の説明図



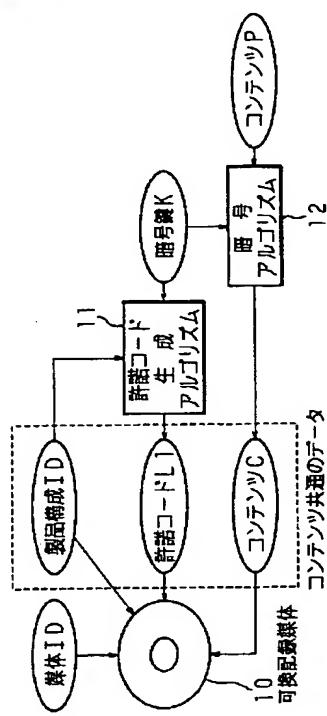
【図12】

第18発明に係る記録媒体の実施の形態の構成を説明する為の説明図



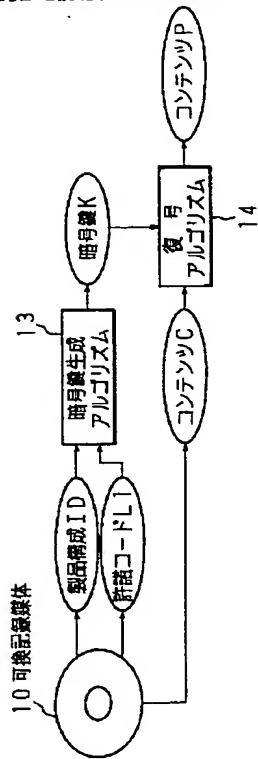
〔図1〕

第1、2発明に係る再生許可方法、第11発明に係る記録方法及び第14、15発明に係る記録媒体の実施の形態1を説明するための説明図



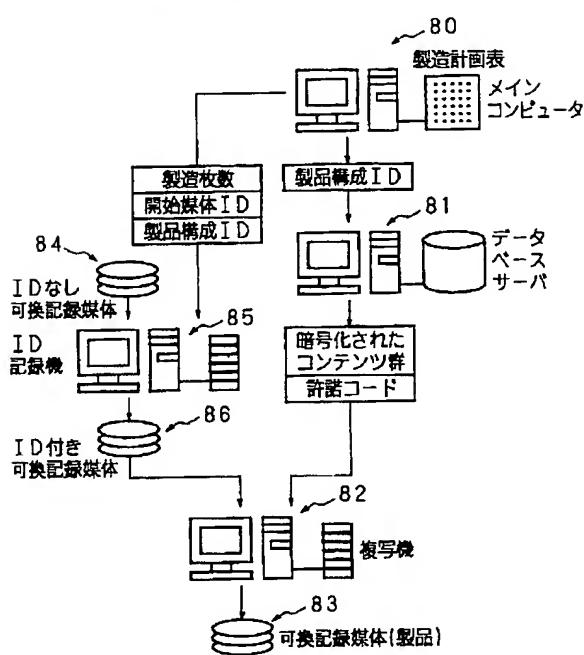
[図2]

可換記録媒体に記録されたコンテンツの利用方法を説明するための説明図



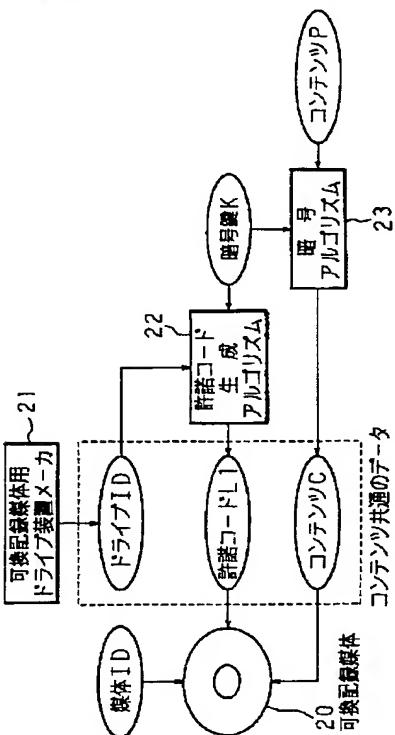
【図3】

可換記録媒体の製造工程を説明する為の説明図



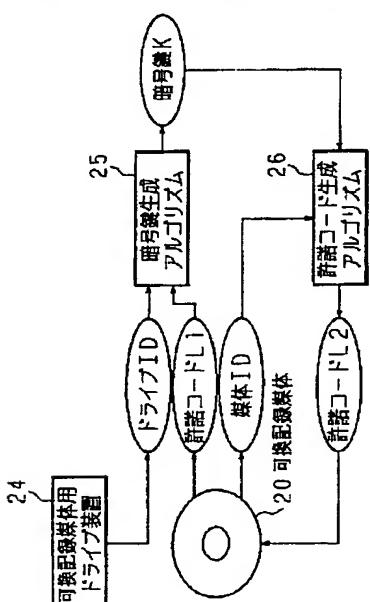
【図4】

第3～5、8～10発明に係る再生許可方法、第12発明に係る記録方法及び第16発明に係る記録媒体の実施の形態2を説明する為の説明図



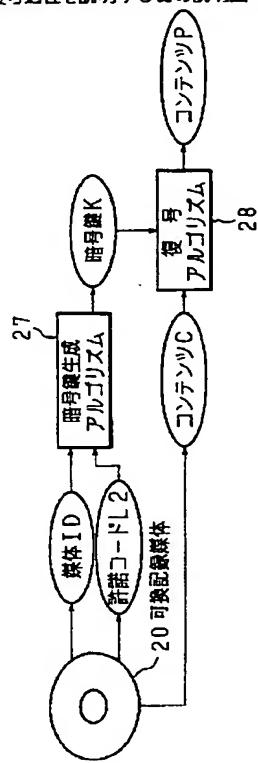
【図5】

可換記録媒体に記録されたコンテンツが初めて利用される前に行われる許諾コードの変更方法を説明する為の説明図



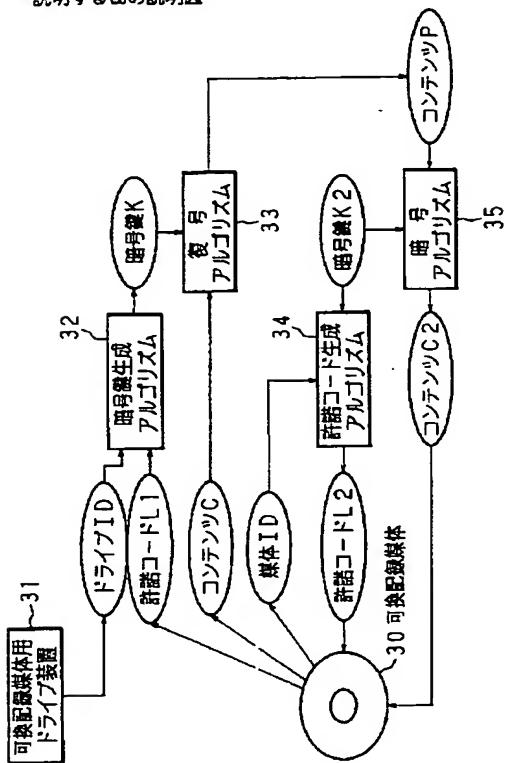
【図6】

許諾コードL2が可換記録媒体に記録された後に行われる
コンテンツの復号過程を説明するための説明図



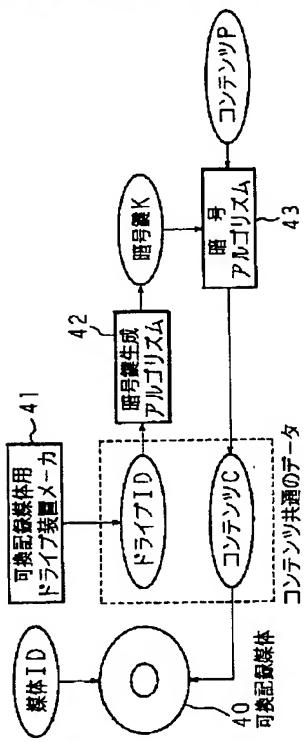
【図7】

許諾コードの変更方法及びコンテンツの再暗号化を
説明するための説明図



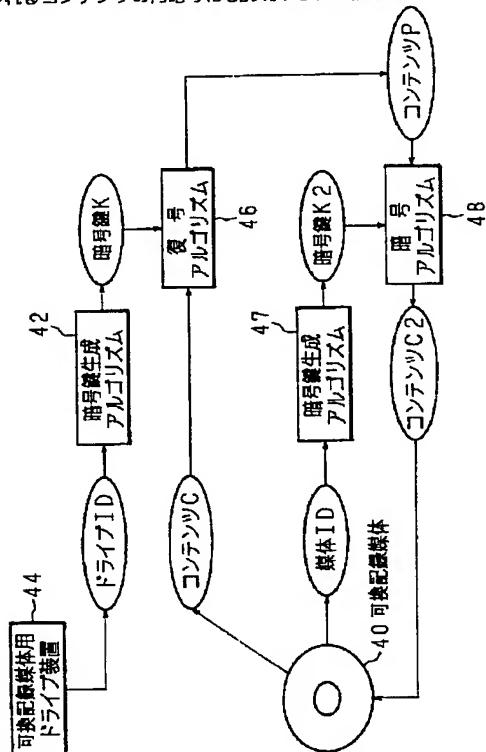
[図8]

第3, 7, 8発明に係る再生許可方法及び第13発明に係る記録方法の実施の形態4を説明する為の説明図



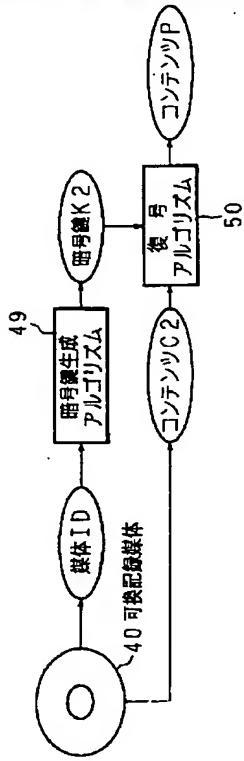
[図9]

可換記録媒体に記録されたコンテンツが初めて利用される前に 行われるコンテンツの再暗号化を説明するための説明図



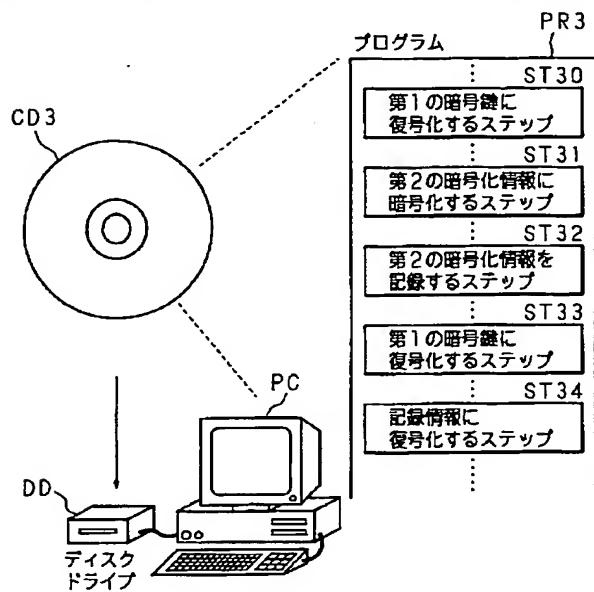
【図10】

再暗号化されたコンテンツが可換記録媒体に記録された後に
行われるコンテンツの復号過程を説明する為の説明図



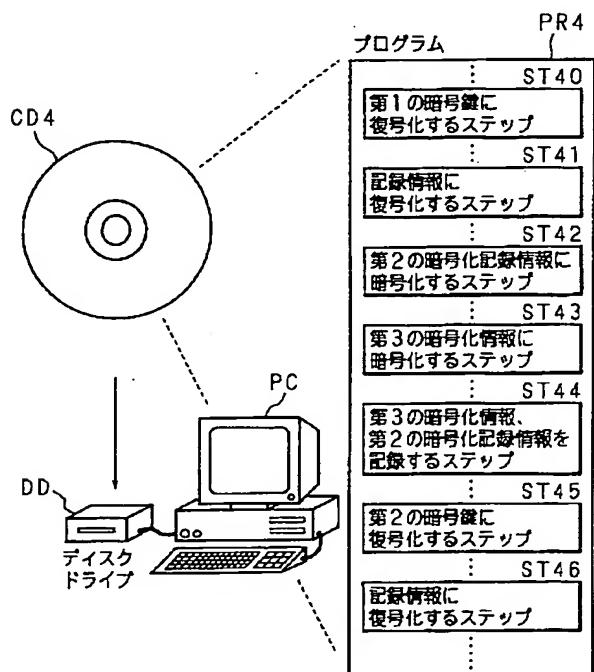
【図13】

第19発明に係る記録媒体の実施の形態の構成を説明する為の説明図



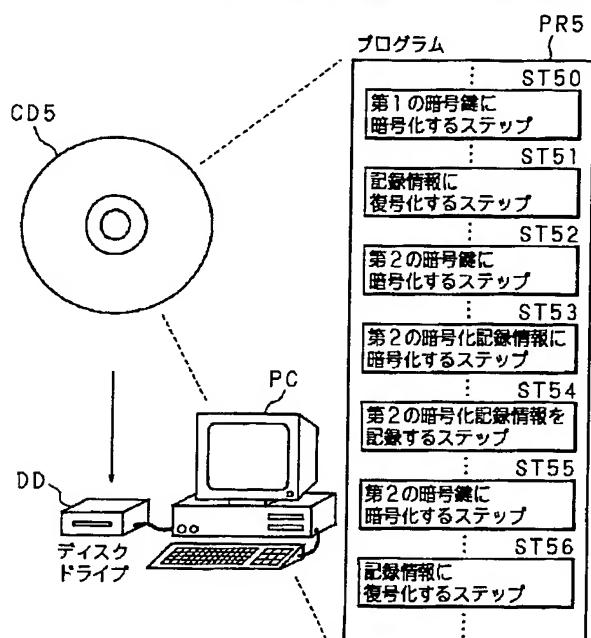
【図14】

第20発明に係る記録媒体の実施の形態の構成を説明する為の説明図



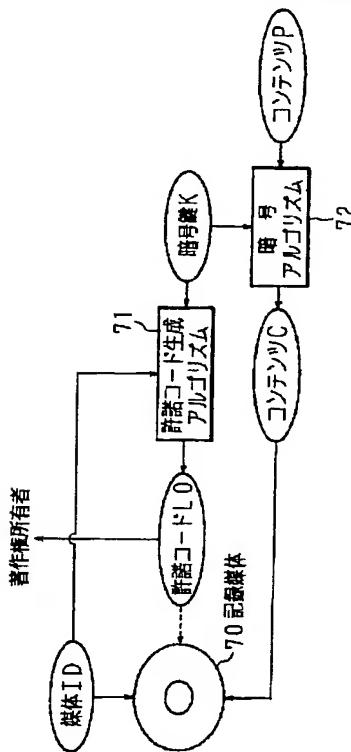
【図15】

第21発明に係る記録媒体の実施の形態の構成を説明する為の説明図



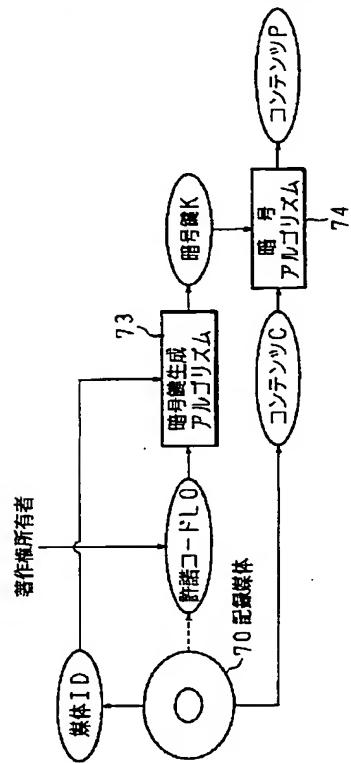
【図16】

従来の再生許可方法の一例を説明する為の説明図



【図17】

従来の再生許可方法の一例を説明するための説明図



THIS PAGE BLANK (cont.)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

...SOME BLANK...